(12) UK Patent Application (19) GB (11) 2 293 737 (13) A

(43) Date of A Publication 03.04.1996

(21) Application No 9519230.8

(22) Date of Filing 20.09.1995

(30) Priority Data
(31) 08326309 (32) 29.09.1994 (33) US

(71) Applicant(s)
Pitney Bowes Inc

(Incorporated in USA - Delaware)

World Headquarters, One Elmcroft, Stamford,
Connecticut 06926-0700, United States of America

(72) Inventor(s)
Leon A Pintsov

(74) Agent and/or Address for Service
Hoffmann Eitle & Partner
Sardinia House, Sardinia Street, 52 Lincolns
Inn Fields, LONDON, WC2A 3LZ, United Kingdom

(51) INT CL^6
H04L 9/30 , G07B 17/02

(52) UK CL (Edition O)
H4P PDCSC
B6C CVSA C1200 C1249 C1271
U1S S2133

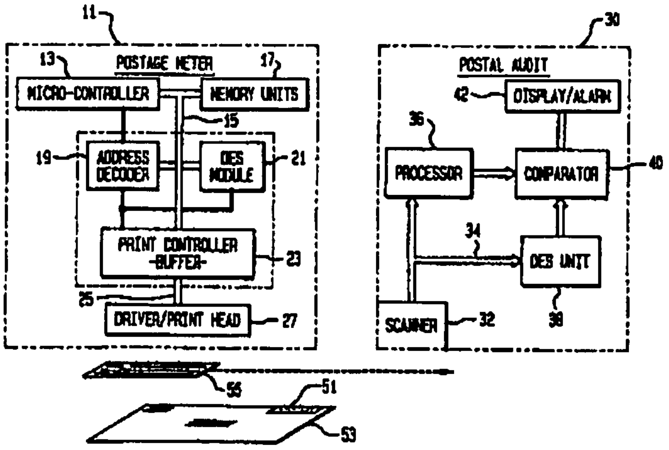
(56) Documents Cited
EP 0647925 A2 EP 0388867 A2 US 5208858 A
US 5073935 A US 4796297 A

(58) Field of Search
UK CL (Edition N) H4P PDCSA PDCSC PDCSX
INT CL^6 G07B 17/04 , H04L 9/30 9/32
Online:WPI,CLAIMS,JAPIO,USPATFULL,INSPEC

(54) Postage evidencing system with encrypted hash summary reports

(57) A method verifyies summary activity report representing the total postage expended by a postage meter (11) for a given activity period per preselected postal categories by generating a hash value representative of the postal transactions of the meter. As a first step, each transaction is recorded in the meter memory unit (17). The funding activity records are then retrieved from unit (17) by recorded postal category for the selected activity period. A hash value is then calculated for the retrieved records. The calculated hash value is encrypted and printed along with the retrieved record of funding activity. The printed report including the encrypted hash value is then inputted into a verification apparatus (30) by either key entry or optical scanner (32). The verification apparatus (30) then independently calculates a hash value based upon the inputted record of funding activity and generates an encrypted hash value representative of the inputted funding information. A comparison is made between the now derived encrypted hash value and the encrypted hash value generated by said verification apparatus. If the report has not been altered the encrypted hash values will be identical.

FIG. 1



GB 2 293 737 A

FIG. 1

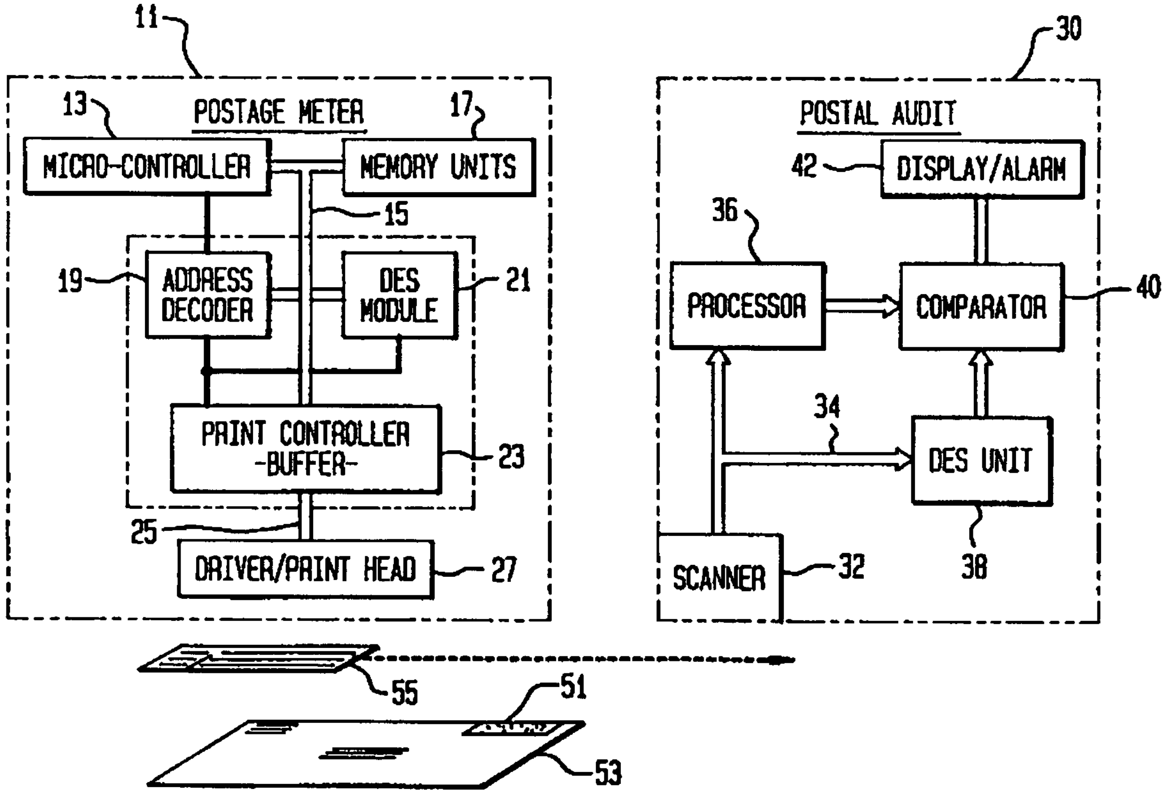

11
POSTAGE METER
13
MICRO-CONTROLLER
17
MEMORY UNITS
15
19
ADDRESS DECODER
DES MODULE
21
PRINT CONTROLLER -BUFFER-
23
25
DRIVER/PRINT HEAD
27
55
51
53
30
POSTAL AUDIT
42
DISPLAY/ALARM
36
PROCESSOR
COMPARATOR
40
34
DES UNIT
SCANNER
32
38

FIG. 2

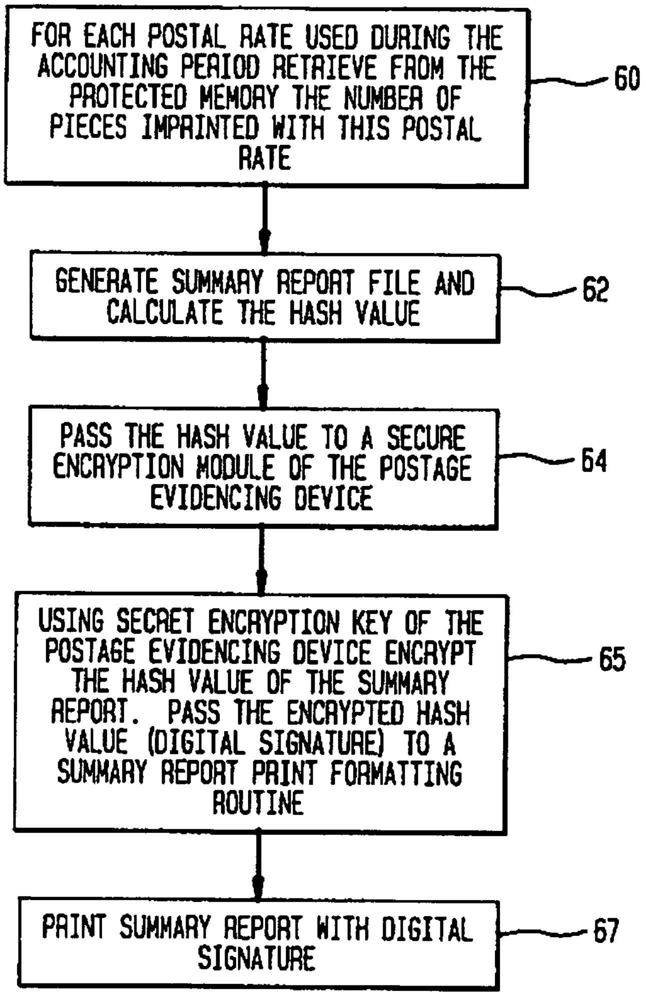
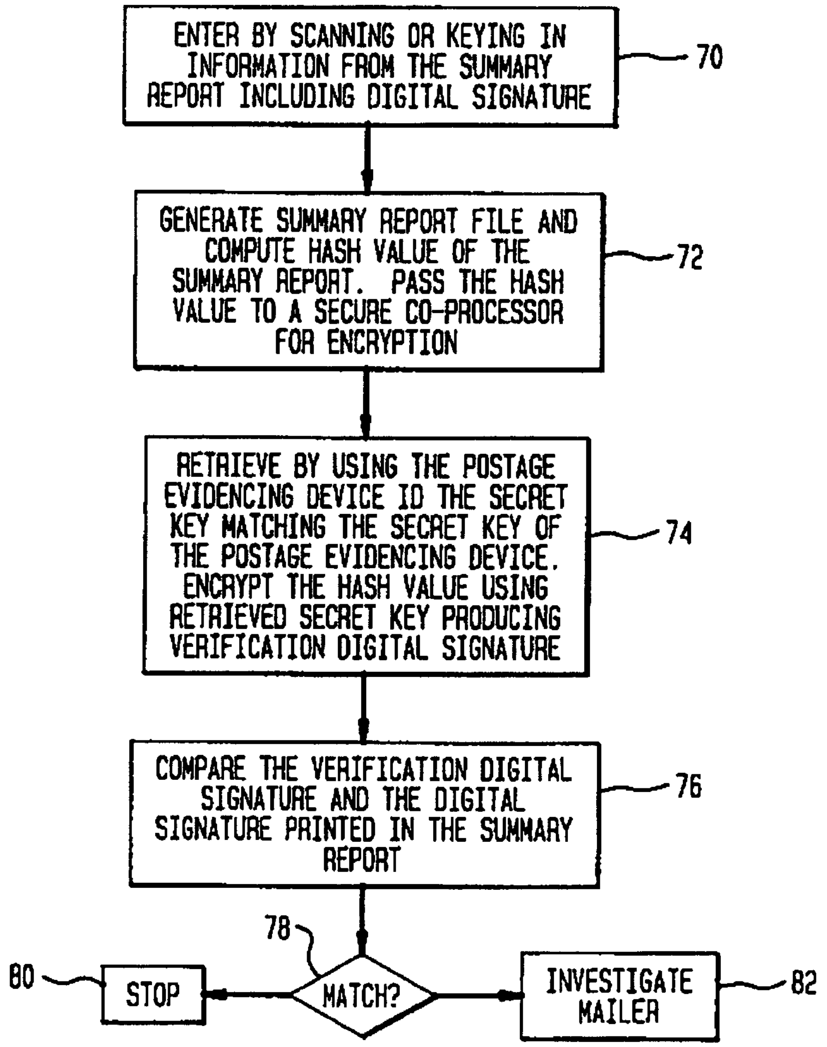

FOR EACH POSTAL RATE USED DURING THE ACCOUNTING PERIOD RETRIEVE FROM THE PROTECTED MEMORY THE NUMBER OF PIECES IMPRINTED WITH THIS POSTAL RATE
60
GENERATE SUMMARY REPORT FILE AND CALCULATE THE HASH VALUE
62
PASS THE HASH VALUE TO A SECURE ENCRYPTION MODULE OF THE POSTAGE EVIDENCING DEVICE
64
USING SECRET ENCRYPTION KEY OF THE POSTAGE EVIDENCING DEVICE ENCRYPT THE HASH VALUE OF THE SUMMARY REPORT. PASS THE ENCRYPTED HASH VALUE (DIGITAL SIGNATURE) TO A SUMMARY REPORT PRINT FORMATTING ROUTINE
65
PRINT SUMMARY REPORT WITH DIGITAL SIGNATURE
67

FIG. 3


ENTER BY SCANNING OR KEYING IN INFORMATION FROM THE SUMMARY REPORT INCLUDING DIGITAL SIGNATURE
70
GENERATE SUMMARY REPORT FILE AND COMPUTE HASH VALUE OF THE SUMMARY REPORT. PASS THE HASH VALUE TO A SECURE CO-PROCESSOR FOR ENCRYPTION
72
RETRIEVE BY USING THE POSTAGE EVIDENCING DEVICE ID THE SECRET KEY MATCHING THE SECRET KEY OF THE POSTAGE EVIDENCING DEVICE. ENCRYPT THE HASH VALUE USING RETRIEVED SECRET KEY PRODUCING VERIFICATION DIGITAL SIGNATURE
74
COMPARE THE VERIFICATION DIGITAL SIGNATURE AND THE DIGITAL SIGNATURE PRINTED IN THE SUMMARY REPORT
76
78
80
STOP
MATCH?
INVESTIGATE MAILER
82

POSTAGE EVIDENCING SYSTEM WITH SECURE SUMMARY REPORTS

The present invention relates to funding apparatus such as postage evidencing devices and, more particularly, to postage meters having an accounting system and means for communicating account records.

Conventional postage meters utilize letter press techniques to print a postage payment indicia on an envelope as evidence of postage payment and a secure accounting system for recording postage dispensed. A number of security methods have been devised over time to protect against fraudulent printing of postage indicia with respect to letter press type postage meters. For example, special inks are used, and the indicia plate and postage value print wheels are physically secured to prevent an unauthorized indicia impression from being taken. As noted, the conventional postage meter accounts for the postage printed by the postage meter and a number of methods have been devised to protect the postage accounting system within the meter, e.g., tamper proof housings.

Postage evidencing devices, such as the conventional postage meters, are now being developed utilizing digital printing techniques, such as thermal transfer printing. Digital printing techniques employ bit map addressable printing which differs significantly from traditional letter press printing. The critical security provision for digitally printed indicia is by encrypted information such as digital tokens, for example, as described in detail in US Patent No. 5,448,641, entitled POSTAL RATING SYSTEM WITH VERIFIABLE INTEGRITY, which describes a procedure for providing postal rate security. Encrypted information verification requires either a secret key or a public key encryption system. It has been concluded that a secret key system is more advantageous for the mailer-post communication. Any secret key cryptographic system assumes the presence of a secret key shared by the particular postage meter provided and the verification authority, usually the Postal Service.

A potential benefit of digital printing postage meter devices is the ability to utilize the digital printer for printing both the postage indicia and to use the same digital printer to print, on request, a summary report of metering activities during some pre-specified accounting period.

The summary report preferably would contain a table of data including number of mailpieces in different rate categories and associated postage, plus a total postage printed during the accounting period. The summary report can be printed preferably by the postage meter digital printer which is used to print the postage indicia or by any other printer attached to a computer (PC) equipped with a standard serial interface, e.g., RS 242. In the latter case, the summary data is passed to the PC through the RS 242 interface of the postage meter.

The summary report can be audited by the Postal Service in order to compare their records of mailing activities of the postage meter by serial number or other identifying number and mailer's records. The total postage spent is usually stored in a protected tamper resistant memory of the postage meter and it would be detectable if the mailer would try to alter this number. However, the other parts of the report can be easily altered without changing the total postage spent. Because of the characteristics of the postal rating structure, the total number of pieces as well as the number of pieces by class/weight can be fraudulently decreased in the report thus misleading the auditing authority of the Postal Service to the benefit of the mailer.

Summary of the Invention

It is the objective of the present invention to provide a method such that unauthorized alteration of the summary mail report is detectable by the postal auditing authority using cryptography means.

The summary report data is subjected to a conventional cryptographic hash function. The value of the hash function represents a "fingerprint" of the summary report. Thus, any attempt to alter any character in the summary report would result in a change in the value of the hash function. Once a hash value of the summary report file is computed, it can be encrypted with the same secret key which the postage evidencing device utilizes for encrypting information printed in the indicia (i.e., digital tokens). Then the encrypted value of the hash function is printed together with the summary report, in effect providing a digital signature that authenticates the summary report information. In this case, the summary report could have the appearance as represented in Table 1.

Table 1 - Signed Summary Report

Postage Evidencing Device ID: 12345678
Accounting Period: June 1, 1994 -- July 1, 1994

Mail Category/Weight	Number of Pieces	Postage/Piece	Postage
Class 1-1oz	10	$0.29	$2.9
Class 1-2oz	7	$0.52	$3.64
Class 3-1oz	20	$0.19	$3.80
Class 4-60oz	5	$1.07	$5.35
Total	42	N/A	$15.69

Digital Signature: 12309876552344567890998776654233445.

The relevant for summary report data should be stored in a protected tamper resistant memory. This data includes number of pieces in each category that were imprinted by the postage evidencing device. Once this data is properly stored, the summary report is generated with this data and digitally signed in a manner which cannot be altered undetectably.

Brief Description of the Drawings

Fig. 1 is a schematic of a micro control system for driving a thermal transfer digital printing postage meter and a computer base system in accordance with the present invention.

Fig. 2 is a flow chart illustrating an activity report generation process in accordance with the present invention.

Fig. 3 is a flow chart illustrating the auditing process for verifying the activity report generated in accordance with the present invention.

Detailed Description of the Preferred Embodiment

Referring to Fig. 1, a postage meter 11 is comprised of a microcontroller 13 in bus 15 communication with memory units 17, address decoder 19, encryption and decryption module (DES) 21 and a printer controller/buffer unit 23, all of any suitable design. The printer controller/buffer unit 23 is in bus 25 communication with any suitable thermal print driver and suitable print head 27. It is intended that the postage meter be of any suitable design for employing digital printing techniques, such as ink jet, laser or thermal transfer.

A postal audit unit 30 is comprised of a scanner/optical character reader 32 of any suitable conventional design to provide input to the postal audit system 30. Alternatively, a keyboard input unit (not shown) may be used. Preferably, the scanner 32 is in bus 34 communication with a processor unit 36 and encryption and decryption unit (DES) 38. The processor unit 36 and encryption and decryption unit (DES) 38, respectively, provide input to a comparator 40. The output from the comparator 40 is directed to a conventional display/alarm unit 42.

The postage meter is intended to print postage payment indicia 51 on an envelope 53 in any one of known methods. In a manner to be described in greater detail subsequently, the meter is programmed to maintain a record of the posting characteristics, such as, class, weight and amount of postage dispensed per mailpiece in the memory units in any suitable known manner.

The microcontroller 13 of the postage meter 11 is further programmed in any suitable conventional manner to generate account reports pursuant to the posting characteristics information stored in memory and to print a report 55 utilizing the meter print head 27. The report will also include a digital signature derived in a manner subsequently described. It should also be appreciated that alternatively by utilizing a communication port of the postage meter (not shown), a conventional computer may be interfaced to the postage meter in a conventional manner such that the report, along with the digital signature, can be electronically transferred to the computer for printing under the control of the computer (not shown).

In the preferred embodiment, the report 55 is printed under the control of the postage meter microcontroller 13 and transferred to the postal service postal audit unit 30. The information from the report 55 may be keyed in from a keyboard (not shown) or, preferably, placed under a scanner 32 containing an optical character reader (OCR). The scanner 32 then transfers the information derived from scanning the report 55 to the processor 36 and DES unit 38 along a bus 34. The information processed in the processor 36 and the DES unit 38, in a manner subsequently described, and is compared by a comparator 40 with the information printed in the report. The output from the comparator 40 is directed to the display 42 which may include an alarm for actuation depending on the output of the comparator 40.

The microprocessor 13 is programmed to apply a hash function to the account information data to produce a hash value which is indicative of the content of the summary report and yet may be considerably reduced in data size. As used herein, hash function is a well-known function which possesses at least two properties. It is computationally difficult to (i) recover a message corresponding to a given message digest and (ii) to find two different messages which produce the same hash value (message digest). Some well-known hash functions are described in American National Standard X9.30 - 1993, Public Key Cryptography Using Irreversible Algorithms For The Financial Services Industry: Part 2: The Secure Hash Algorithm (SHA). It should be noted that there are other publicly available hash functions that can be implemented for the purpose of the present invention. As for example, one formal definition is set forth in Contemporary Cryptology by G. Simmons, IEEE Press 1992 at page 345, and yet another definition is that a hash function is a function that satisfies the following properties:

1) it is capable of converting a file F of arbitrary length into a fixed-length digest h (F);
2) h must be "one way", that is, given an arbitrary value y in the domain of h, it must be computationally infeasible to find file F such that h (F) = y; and
3) h must be "collision free", that is, it must be computationally infeasible to construct two different files F_1 and F_2 such that
$h(F_1), = h(F_2)$

If the data (the summary report data) being transmitted to the postal audit unit 42 is not private, it is not necessary to encrypt the information and prevent unauthorized decryption i.e., it is not important to protect secrecy of the information itself otherwise this information can be suitably encrypted. Upon calculation of the hash value of the summary report data, the postage evidencing device encrypts the hash value, with its secret key and prints the encrypted message in the report. The postal audit unit 30 receives the encrypted hash value ("signature") (e.g. by OCR scanning), and decrypts it with a secret key shared with the postage evidencing device, thus obtaining the plain text hash value. The postage audit unit 30 then independently computes the hash value of the received summary report data using the same hash function as was used by the postage evidencing device. The hash algorithm employed may be one in the public domain. However, the algorithm resides both at the postage evidencing device 11 and at the postal audit unit 30. If the two hash values, namely the hash value computed in the postage evidencing device 11 and audit unit 30 match each other, the integrity of the summary report data 55 is assured. Alternatively, you can generate just the digital signature and compare. Whether the alternative is preferred depends on whether the encryption/decryption is symmetrical or not.

Referring now to Fig. 2, the microcontroller 13 is programmed to generate summary report by entering a report routine. The report routine, at process block 60, retrieves from the protected memory for each postal rate used during the accounting period, the number of pieces imprinted with this postal rate. At process block 62, a summary report file is generated and the hash value of this file is calculated. At process block 64, this hash value is passed to a secure encryption module 21 of the postage evidencing device micro control system. At process block 65, using secret encryption key of the postage evidencing device, the hash value of the summary report is encrypted and the encrypted hash value (digital signature) is prepared for printing. Finally, at logic block 67, the summary report with digital signature is printed.

Auditing of the summary report can be done by essentially repeating the same steps, namely computing the hash value of the summary report as printed using the same hashing algorithm as was used to create the digital signature by the postage evidencing device. Then the hash value is encrypted with the same secret key which is shared between the post office audit system and the postage meter. Finally, the resulting encrypted value is compared with the digital signature printed in the summary report. A mismatch indicates alteration of the summary report. A match assures that the report has not been altered.

The auditing process is depicted in the following Fig. 3. At process block 70, information from the summary report including digital signature is entered by either scanning or keying the information into the audit unit 30. At process block 72, summary report file is generated and the hash value of that summary report is computed and passed to a secure processor 38 for encryption. At process block 74, the secret key matching the secret key of the postage meter is retrieved by using the postage meter ID and the encrypted hash value using retrieved secret key produces a verification digital signature. At decision process block 76, the digital signature printed in the summary report and the verifying digital signature are compared. If they match at process block 78, then the process terminates at process block 80. If they do not match at process block 78, then the auditor is alerted to investigate mailer at process block 82.

Claims:

1. A method of verifying an activity report representing the funding activity of a funding apparatus for a given activity period by a verification apparatus, said funding apparatus having a microcomputer system programmed to track and record funding activity of the funding apparatus by funding category in a memory unit comprising the steps of:

retrieving from said memory unit said record of funding activity of said funding apparatus for said activity period;

calculating a hash value for said retrieved record of funding activity;

encrypting said calculated hash value;

printing said retrieved record of funding activity and said encrypted hash value;

inputting said printed record of funding activity into said verification apparatus, said verification apparatus having means for calculating a hash value based upon said inputted record of funding activity and generating an encrypted hash value from said calculated hash value; and

comparing said printed encrypted hash value with said encrypted hash value generated by said verification apparatus.

2. A method as claimed in claim 1 wherein said encryption steps incorporate a encryption key unique to said particular funding apparatus.

3. A method as claimed in claim 1 or 2 wherein said funding apparatus is a postage meter.

4. A method of verifying a summary activity report representing the total postage expended by a postage meter funding apparatus for a given activity period for a given postal category by a verification apparatus, said postage meter funding apparatus having a microcomputer system programmed to track and record funding activity of the funding apparatus by postal category in a memory unit comprising the steps of:

retrieving from said memory unit said record of funding activity by postal category of said postage meter funding apparatus for said activity period;

calculating a hash value for said retrieved record of funding activity;

encrypting said calculated hash value;

printing said retrieved record of funding activity and said encrypted hash value;

inputting said printed record of funding activity into said verification apparatus, said verification apparatus having means for calculating a hash value based upon said inputted record of funding activity and generating an encrypted hash value from said calculated hash value; and

comparing said printed encrypted hash value with said encrypted hash value generated by said verification apparatus.

5. A method as claimed in claim 4 wherein said encryption steps incorporate a encryption key unique to said particular postage meter funding apparatus.

6. A method of verifying a summary activity report representing the total postage expended by a postage meter funding apparatus for a given activity period for a given postal category by a verification apparatus, said postage meter funding apparatus having a microcomputer system programmed to track and record funding activity of the funding apparatus by postal category in a memory unit comprising the steps of:

retrieving from said memory unit said record of funding activity by postal category of said postage meter funding apparatus for said activity period;

calculating a hash value for said retrieved record of funding activity;

encrypting said calculated hash value;

printing said retrieved record of funding activity and said encrypted hash value;

inputting said printed record of funding activity and said encrypted hash value into said verification apparatus, said verification apparatus having means for calculating a hash value based upon said inputted record of funding activity and decrypting said encrypted hash value; and

comparing said decrypted hash value with said calculated encrypted hash value generated by said verification apparatus.

7. A method as claimed in claim 6 wherein said encryption steps incorporate a encryption key unique to said particular postage meter funding apparatus.

8. Funding apparatus comprising: a microprocessor system for tracking and recording funding activity; a memory unit for storing funding data; means for calculating a hash value in respect of the funding data; means for encrypting the hash value; and means for printing the encrypted hash value.

9. Apparatus according to claim 8 wherein said printing means is further arranged to print the funding data.

10. Verification apparatus comprising: means for entering a record of funding activity and an encrypted hash value calculated therefrom; means for calculating a hash value from said record; means for generating an encrypted hash value from the calculated has value; and
means for comparing said encrypted hash value with said entered encrypted hash value.

11. A method of verifying an activity report substantially as hereinbefore described with reference to the accompanying drawings.

12. Funding apparatus substantially as hereinbefore described with reference to the accompanying drawings.

13. Verification apparatus substantially as hereinbefore described with reference to the accompanying drawings.

10

Patents Act 1977 **Examiner's report to the Comptroller under Section 17** **(The Search report)**	Application number GB 9519230.8
Relevant Technical Fields (i) UK Cl (Ed.N) H4P PDCSA, PDCSC, PDCSX (ii) Int Cl (Ed.6) G07B 17/04, H04L 9/30, 9/32	Search Examiner MR B J SPEAR Date of completion of Search 22 NOVEMBER 1995
Databases (see below) (i) UK Patent Office collections of GB, EP, WO and US patent specifications. (ii) ONLINE: WPI, CLAIMS, JAPIO, USPATFULL, INSPEC	Documents considered relevant following a search in respect of Claims :- 1-13

Categories of documents

X:	Document indicating lack of novelty or of inventive step.	P:	Document published on or after the declared priority date but before the filing date of the present application.
Y:	Document indicating lack of inventive step if combined with one or more other documents of the same category.	E:	Patent document published on or after, but with priority date earlier than, the filing date of the present application.
A:	Document indicating technological background and/or state of the art.	&:	Member of the same patent family; corresponding document.

Category	Identity of document and relevant passages		Relevant to claim(s)
XP	EP 0647925 A2	(PITNEY BOWES) whole document, eg page 4 lines 57-58, page 7 lines 12-45 and Figures 1-3	8, 10 at least
XY	EP 0386867 A2	(FISCHER) whole document, eg page 11 line 27 - page 12 lines 5, Figures 2, 3, 8-12	1, 2, 4, 6, 8, 9, 10 at least
XY	US 5208858	(SIEMENS) whole document, eg Figure 1 and column 3 line 60 to column 4 line 25	1, 4, 6, 8, 10 at least
Y	US 5073935	(PASTOR) whole document, eg Figure 2 and column 4 lines 29-47	8, 10 at least
Y	US 4796297	(NEC) whole document, eg column 4 lines 12-33, column 9 lines 39-59	8, 10 at least

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).